UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,426	02/28/2002	Lauri Paatero	944-005.5	6252

4955 7590 04/06/2007

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
HERRING, VIRGIL A	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/090,426	PAATERO, LAURI	
	Examiner	Art Unit	
	Virgil Herring	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27,35-43 and 45-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27,35-43 and 45-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the amendment filed 8 January 2007. Claims 28-34 and 44 were previously cancelled. Claims 1-27, 35-43, and 45-50 are currently pending.

Response to Arguments

Applicant's arguments with respect to the reference to the Hind patent have been considered but are moot in view of the new ground(s) of rejection, which do not include these references.

Applicant's arguments filed 8 January 2007 with respect to the rejections based on the Doyle patent have been fully considered but they are not persuasive.

Regarding independent claims 1, 20, 26, 41, and 49, applicant argued that Doyle does not disclose the limitation that "the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device," because "before the operably connected components are connected to the portable device, there is no relationship or communication at all between Doyle's portable device and the certificates associated with the components." The examiner respectfully disagrees, noting that while the communication does not take place before the components are connected, the certificates must already be in the components. The examiner reached this conclusion based on, for example, column 9, lines 32-34.

The components are authenticated after being connected to the secure core, which indicates that a certificate is already present, to allow the authentication to take place.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-27, 35-43, and 45-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Doyle et al (US Patent #6,968,453).

With regards to claim 1, Doyle et al disclose a method, comprising:

embedding a role certificate in a device, wherein the role certificate identifies at least one permitted activity that at least one party is allowed to perform with respect to the device, and wherein the role certificate is generated by a Certification Authority (CA); (note figure 1 and associated description; note column 9, line 54; note column 7, lines 13-17; note column 11, lines 8-40; note figures 4 & 6)

embedding at least information regarding a public key in said device the public key corresponding to the private key used by the CA to sign the role certificate; and (note figure 1 and associated description; note column 9, line 54; note column 8, lines 1-30; note column 9, lines 46-67; note column 7, lines 13-17; note column 11, lines 8-40; note figures 4 & 6)

running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party if the role certificate is verified, (note figure 1 and associated description; note column 5, lines 1-24; note column 6, lines 28-37; note column 11, lines 8-40; note figures 4 & 6)

wherein the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device. (see arguments above; note column 11, lines 8-40 – third party upgrading implies communication with the third party)

With regards to claims 20 and 49, Doyle et al disclose a role certificate mechanism, comprising:

memory within containing a role certificate, wherein the role certificate is configured to identify at least one activity permitted to be activated within a device in response to a communication, and further wherein the memory contains information regarding a first key corresponding to a second key used to sign the role certificate; and (note figure one and associated description; note column 7, lines 13-17; note figures 4 & 6)

processor configured to run the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device, (note figure one and associated description; note column 5, lines 1-24; note figures 4 & 6)

wherein the role certificate mechanism is configured to receive the communication only after the role certificate is embedded in said mechanism. (see arguments above; note column 11, lines 8-40 – third party upgrading implies communication with the third party)

With regards to claim 26, Doyle et al disclose an apparatus, comprising:

means for embedding a role certificate in a device, wherein the role certificate identifies at least one permitted activity that is allowed to be performed by at least one party with respect to the device, and wherein the role certificate is generated by a Certification Authority (CA); (note figure 1 and associated description; note column 5, lines 3-5; note column 6, lines 46-54; note column 7, lines 13-17; note figures 4 & 6)

means for embedding information regarding a public key in said device, the public key corresponding to the private key used by the CA to sign the role certificate; and(note figure 1 and associated description; note column 5, lines 47-52; note column 9 , lines 46-67; note column 18, lines 66-67 and column 19, lines 1-34)

means for running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party; (note figure 1 and associated description; note column 6, lines 28-37; notes column 7, lines 1-17; note figures 4 & 6)

wherein the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device. (see arguments above; note column 11, lines 8-40 – third party upgrading implies communication with the third party and the device can be manufactured to include a generic role certificate)

With regards to claim 41, Doyle et al disclose a method comprising:

embedding a role certificate applicable to a plurality of devices in an individual device, wherein the role certificate specifies at least one permitted activity that is allowed to be performed by at least one party as applied to the plurality of devices, and wherein the role certificate is generated by a Certification Authority (CA); (note figure 1 and associated description; note column 5, lines 1-5; note column 7, lines 13-17; note column 9, lines 46-67; note column 12)

embedding at least information regarding a public key applicable to the plurality of devices in said individual device, the public key corresponding to the private key used by the CA to sign the role certificate; and (note figure 1 and associated description; note column 5, lines 1-5; note column 7, lines 13-17; note column 9, lines 46-67; note column 12)

running the individual device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the individual device by said at least on party if the role certificate is verified, (note figure 1 and associated description; note

column 5, lines 1-5; note column 7, lines 133-17; note column 9, lines 46-67; note column 12; note column 6, lines 28-37)

wherein the at least one party communicates to perform the permitted activity, only after the role certificate is embedded in said individual device. (see arguments above; note column 11, lines 8-40 – third party upgrading implies communication with the third party)

As per claim 2, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate includes information regarding a control security level for said device so that the device only allows said at least one permitted activity to be a type of action which is within the security level of the device as defined by the role certificate *(note Fig. 1 and associated description in the specification – the secure core 150 is capable of performing the function; also note column 5, lines 1-24; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted; also note column 11, line 18).*

As per claim 3, which is dependent on claim 2, Doyle et al. teaches a method as defined in claim 2, wherein the security level defined by the role certificate allows a type of software code to be downloaded, and/or installed, and/or run on said device by said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-24; also note column 7, lines 13-17 - the certificate is usually generated by CA; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted; also note column 11, line 18).*

As per claim 4, which is dependent on claim 3, Doyle et al. teaches a method as defined in claim 3, wherein the type of software code is from the group of types of software code consisting of test code, production code and special code *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 11, lines 8-40 - third party capability upgrading means described; also note column 11, line 18)*.

As per claim 5, which is dependent on claim 4, Doyle et al. teaches a method as defined in claim 4, wherein the special code can be code linked to a specific at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 11, lines 8-40 - third party capability upgrading means described)*.

As per claim 6, which is dependent on claim 3, Doyle et al. teaches a method as defined in claim 3, wherein the role certificate further contains information with regard to a specific party of said at least one party that can download, and/or install, and/or run said type of software code *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 7, lines 13-17; also note column 5, lines 41-44 - a user profile may contain role information; also note column 11, lines 8-40 - third party capability upgrading means described)*.

As per claim 7, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate further contains information with regard to a specific party of said at least one party that can activate the at least one permitted activity within the device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 8, which is dependent on claim 7, Doyle et al. teaches a method as defined in claim 7, wherein said information with regard to a specific party is a hash of information identifying said specific party's public key, and wherein the device validates said specific party by receiving said information identifying said specific party's public key, and hashing this information and comparing the hash value to the hash value contained in the role certificate so that if the hash values are equal, then the specific party is permitted to activate the at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note Fig. 3 and associated description in the specification; also note column 6, lines 1-27; also note column 11, lines 8-40 - third party capability upgrading means described).*

As per claim 9, which is dependent on claim 7, Doyle et al. teaches a method as defined in claim 7, wherein said specific party is a group of entities *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17; also note column 11, lines 8-40 - third party capability upgrading means described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 10, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the embedding of the role certificate into the device is performed after the information regarding the public key of the CA is embedded into the device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 11, which is dependent on claim 10, Doyle et al. teaches a method as defined in claim 1, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof; also note column 11, line 5).*

As per claim 12, which is dependent on claim 11, Doyle et al. teaches a method as defined in claim 11, wherein the tamper resistant area of the device is a portion memory in the device such that any modification of information stored therein can be ascertained *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof memory; also note column 11, line 5).*

As per claim 13, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected storage can contain certificates that perform the function using the I/O port; also note column 7, lines 13-17 - the digital certificate may contain the stated information; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 14, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the CA is a root CA *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 9, lines 46-67; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 15, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the device is a wireless device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-31; also note column 2, lines 19-41).*

As per claim 16, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the CA is any entity other than said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note Fig. 4; multiple entity can connect via multiple I/O ports or via one port; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 17, which is dependent on claim 1, Doyle et al. teaches a method as defined in claim 1, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17).*

As per claim 18, which is dependent on claim 17, Doyle et al. teaches a method as defined in claim 17, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 13-17).*

As per claim 19, which is dependent on claim 1, Doyle et al. teaches a method as deemed in claim 1, wherein said information regarding the CA public key is a hash value of said CA public key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note Fig. 3)*.

As per independent claim 20, Doyle et al. teaches a role certificate mechanism to permit at least one activity to be activated in a device, comprising:

memory within the device containing a role certificate, wherein the role certificate identifies said at least one activity, and further where the memory contains information regarding a first key corresponding to a second key used to sign the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram such as protected storage 156 that can hold certificate as well as keys; also note also note column 7, lines 13-17; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*; and

means for running the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device *(note Fig. 1 and associated description in the specification – the secure core 150 is capable of performing the function; also note column 5, lines 1-24; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*.

As per claim 21 & 50, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein the memory has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof)*.

As per claim 22, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein the role certificate further includes information regarding the identity of a third party, and wherein the means for verifying the role certificate includes means for reading said third party identity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 8, line 4 – protected area implies tamper proof)*;

wherein the role certificate mechanism further comprises means for receiving information from a third party and comparing at least a portion of said received information with the read third party identity from said role certificate, and if the comparison is the same, allowing said third party to perform said at least one activity on said device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 7, lines 1-16; also note column 6, lines 28-36; also note column 5, lines 25-31)*.

As per claim 23, which is dependent on claim 22, Doyle et al. teaches a role certificate mechanism as defined in claim 22, wherein said device is a mobile phone *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-51; also note column 2, lines 19-41; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*.

As per claim 24, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein said device is a mobile phone *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 1, lines 31-51; also note column 2, lines 19-41; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted)*.

As per claim 25, which is dependent on claim 20, Doyle et al. teaches a role certificate mechanism as defined in claim 20, wherein said information regarding the first key is a hash of said first key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-31; also note column 23, lines 15-67; also note Fig. 3 and associated description in the specification).*

As per claim 27, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate includes information regarding a control security level for said device so that the means for running the device provides that the at least one permitted activity to only be a type of action which is within the security level of the device as defined by the role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 41-44 – a user can be a third party that is allowed to performs a specific role after being authenticated; also note column 6, lines 13-17 - the means for performing the function is described; also note Fig. 4 & Fig. 6 - mechanism for dealing with third party role based functionality is depicted).*

As per claim 35, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 11, line 5 - security core is tamper proof).*

As per claim 36, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein said information regarding the CA public key is a hash of said CA public key *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 6, lines 1-27 and Fig. 3 - the hash technique can be utilized to perform the stated function).*

As per claim 37, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - each certificate can allow different role to include debugging; also note column 5, lines 41-44 - a user can have the privilege to perform the stated function as well)*.

As per claim 38, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the device is a wireless device *(note Fig. 1 and associated description in the specification – the diagram is applicable to cell phone; also note column 6, line 67; also note column 23, lines 5-14; also note column 1, line 39; also note column 3, lines 15-23)*.

As per claim 39, which is dependent on claim 26, Doyle et al. teaches an apparatus as defined in claim 26, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function)*.

As per claim 40, which is dependent on claim 39, Doyle et al. teaches an apparatus as defined in claim 39, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; also note column 8, lines 20-24; also note column 15, lines 6-15)*.

As per claim 42, which is dependent on claim 41, Doyle et al. teaches the method of claim 41, wherein said individual device is also embedded with at least one different role certificate *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12)*.

As per claim 43, which is dependent on claim 42, Doyle et al. teaches method of claim 42, wherein one of the at least one different role certificate specifies at least a third party or a group or a device, and wherein the at least one permitted activity is not conducted if the one of the at least one different role certificate does not match said at least a third party or a group or a device *(note Fig. 1 and associated description in the specification – the functionality can be implemented using the elements depicted in the diagram; also note column 5, lines 1-5; also note column 7, lines 13-17 - the technique described can be used to perform the stated function; note column 9, lines 46-67; also note column 12; also note column 6, lines 28-37)*.

As per claim 45, which is dependent on claim 1, Doyle et al. teaches method of claim 1, wherein one of the role certificate includes a name of the Certification Authority that issued the certificate, a serial number, and an expiration date *(note column 11, line 18)*.

As per claim 46, which is dependent on claim 1, Doyle et al. teaches method of claim 1, wherein the at least one party performs the at least one permitted activity by establishing a wireless connection to the device, and wherein the role certificate also identifies the at least one party *(note column 11, line 18)*.

With regards to claims 47 and 48, Doyle et al disclose the method of claim 1 and mechanism of claim 20, wherein the role certificate is embedded in said device during

manufacture. (column 11, lines 18-40 – the security core that stores the certificates can be manufactured to include a code base providing multiple functionality levels – this is analogous to including a role certificate providing multiple functionality levels when the core is manufactured)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Virgil Herring VH
Examiner
Art Unit 2132

VH

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100